(12) UK Patent Application (19) GB (11) 2 377 057 (13) A

(43) Date of A Publication 31.12.2002

(21) Application No 0208436.6

(22) Date of Filing 12.04.2002

(30) Priority Data
(31) 09681737 (32) 30.05.2001 (33) US

(71) Applicant(s)
Ford Motor Company
(Incorporated in USA - Delaware)
American Road, Dearborn,
Michigan 48121, United States of America

(72) Inventor(s)
Michael Joseph Konopka
Matthew Todd Kromer
Paul L Rathbun

(74) Agent and/or Address for Service
A Messulam & Co. Ltd
43-45 High Road, Bushey Heath, BUSHEY,
Herts, WD23 1EE, United Kingdom

(51) INT CL[7]
G06F 1/00 12/14

(52) UK CL (Edition T)
G4A AAP

(56) Documents Cited
EP 1089516 A2 EP 0992145 A1
WO 2002/012987 A2 WO 2001/025882 A1
US 6339423 A

(58) Field of Search
UK CL (Edition T) G4A AAP
INT CL[7] G06F 1/00 12/14
Other: Online: JAPIO, EPODOC, WPI, TDB, INSPEC, XPESP, IEEEXplore

(54) Abstract Title
Globally restricting client access to a secured web site

(57) A method and system are provided for restricting client access to a web site. A first web server 48 receives a client login 49 and, in response, allocates a cookie to the client 46 containing an access credential 52 having at least one client role-based attribute. A second web server 44 hosts the secured web site 42, web site having an associated security file 50 containing at least one client role-based access privilege. In response to the client's HTTP request at the second server, the cookie is retrieved, decoded and the access credential is compared to the at least one client role-based access privilege. If the access credential has at least one role-based attribute in common with the at least one client role-based access privilege, the client is granted access to the site. Alternately, a site owner defines a token access credential attribute and security file privilege for hierarchal group access to the secured web site.

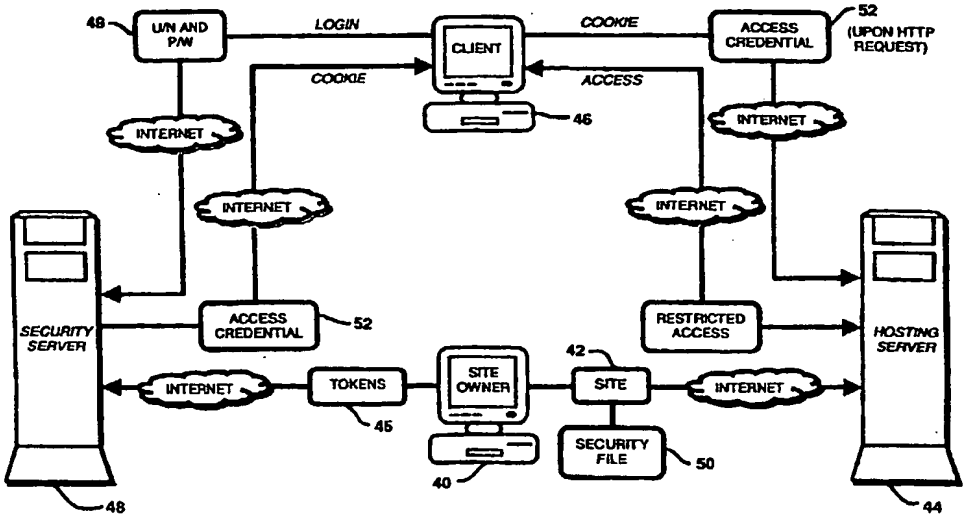

Figure 2

GB 2 377 057 A

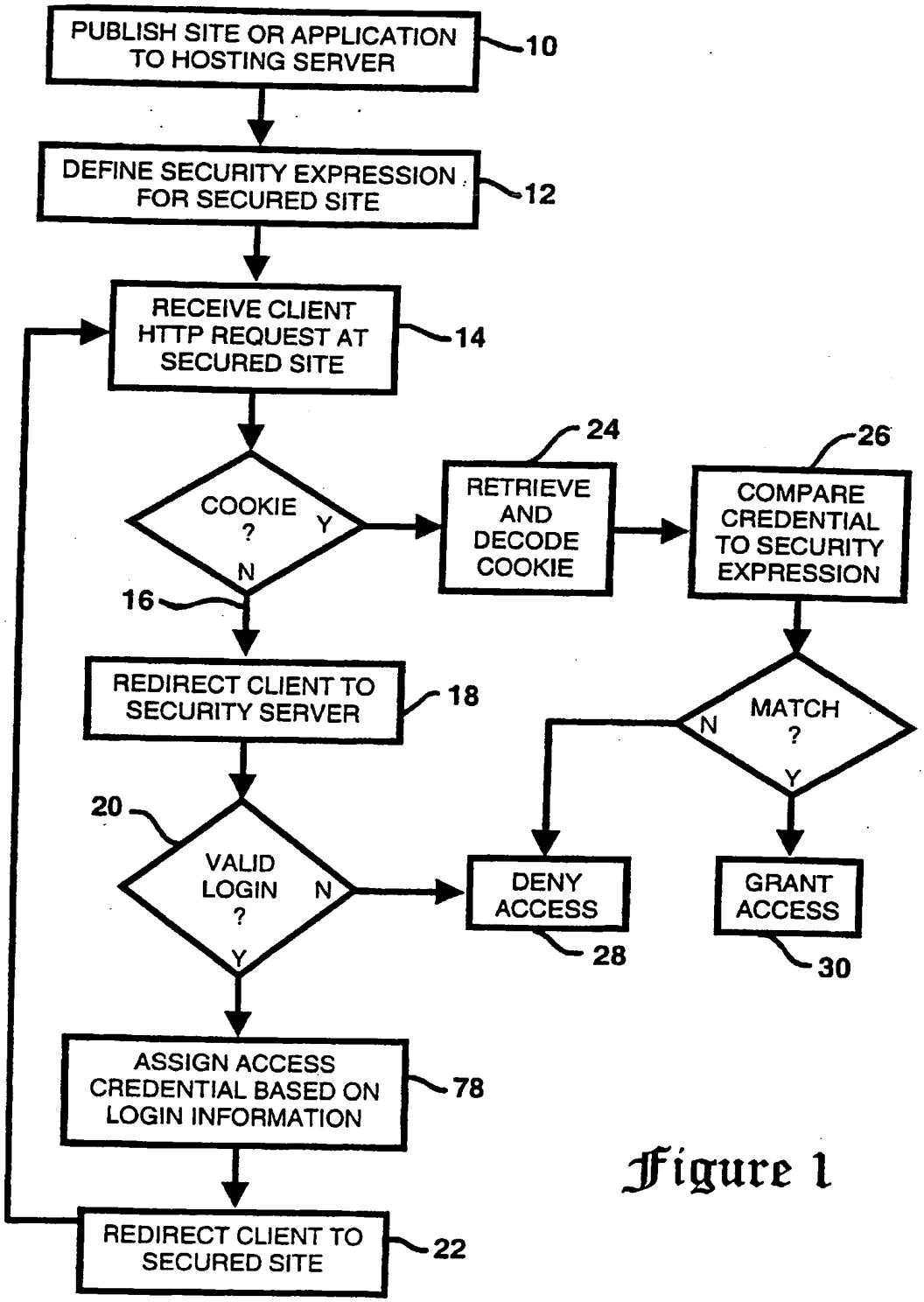
PUBLISH SITE OR APPLICATION TO HOSTING SERVER
10
DEFINE SECURITY EXPRESSION FOR SECURED SITE
12
RECEIVE CLIENT HTTP REQUEST AT SECURED SITE
14
COOKIE ?
Y
N
16
24
RETRIEVE AND DECODE COOKIE
26
COMPARE CREDENTIAL TO SECURITY EXPRESSION
REDIRECT CLIENT TO SECURITY SERVER
18
MATCH ?
N
Y
20
VALID LOGIN ?
N
Y
DENY ACCESS
28
GRANT ACCESS
30
ASSIGN ACCESS CREDENTIAL BASED ON LOGIN INFORMATION
78
REDIRECT CLIENT TO SECURED SITE
22

Figure 1

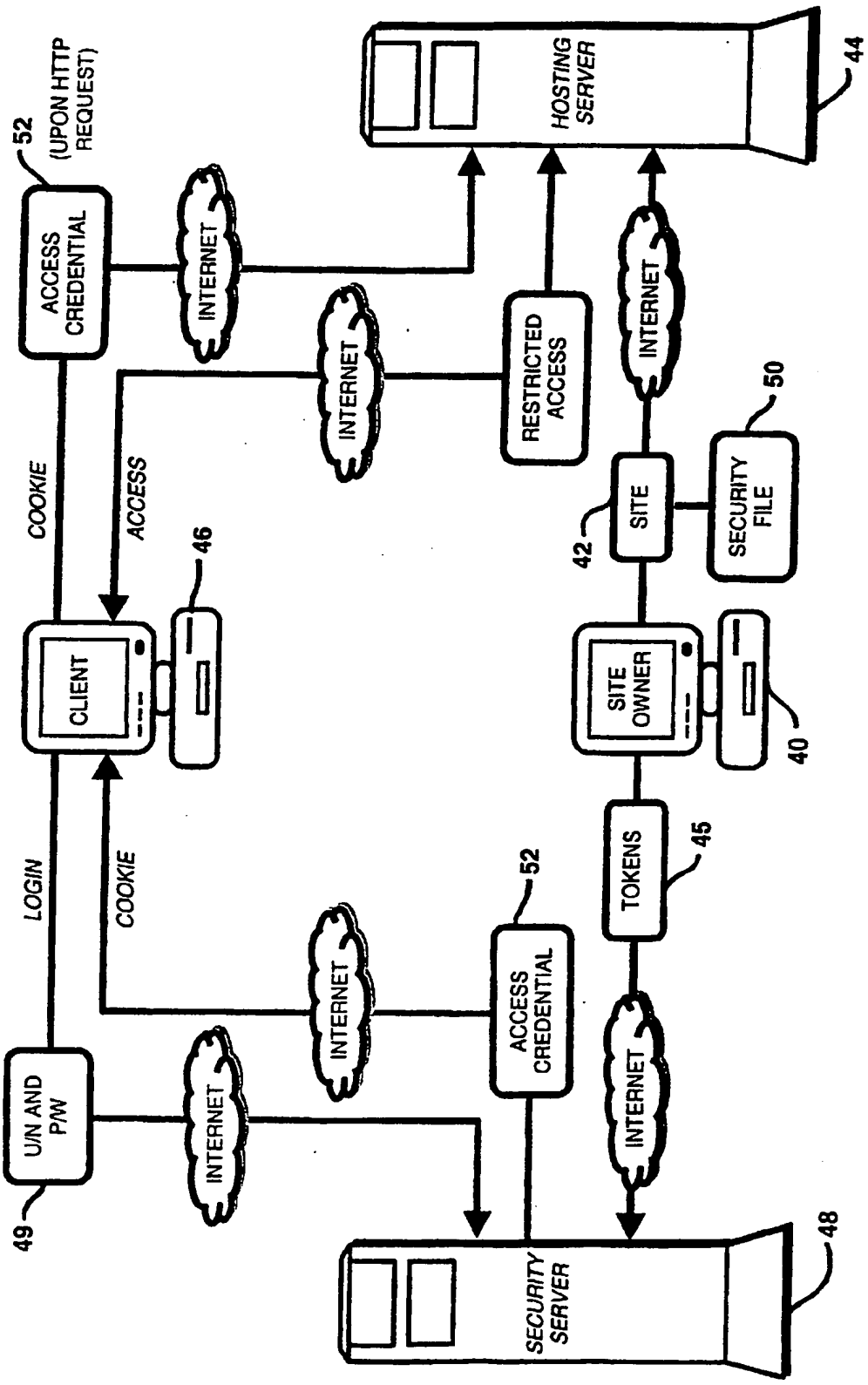
HOSTING SERVER
44
52
(UPON HTTP REQUEST)
ACCESS CREDENTIAL
INTERNET
INTERNET
RESTRICTED ACCESS
INTERNET
COOKIE
ACCESS
46
CLIENT
50
SECURITY FILE
42
SITE
SITE OWNER
40
LOGIN
COOKIE
INTERNET
52
ACCESS CREDENTIAL
TOKENS
45
U/N AND P/W
INTERNET
INTERNET
49
SECURITY SERVER
48

Figure 2

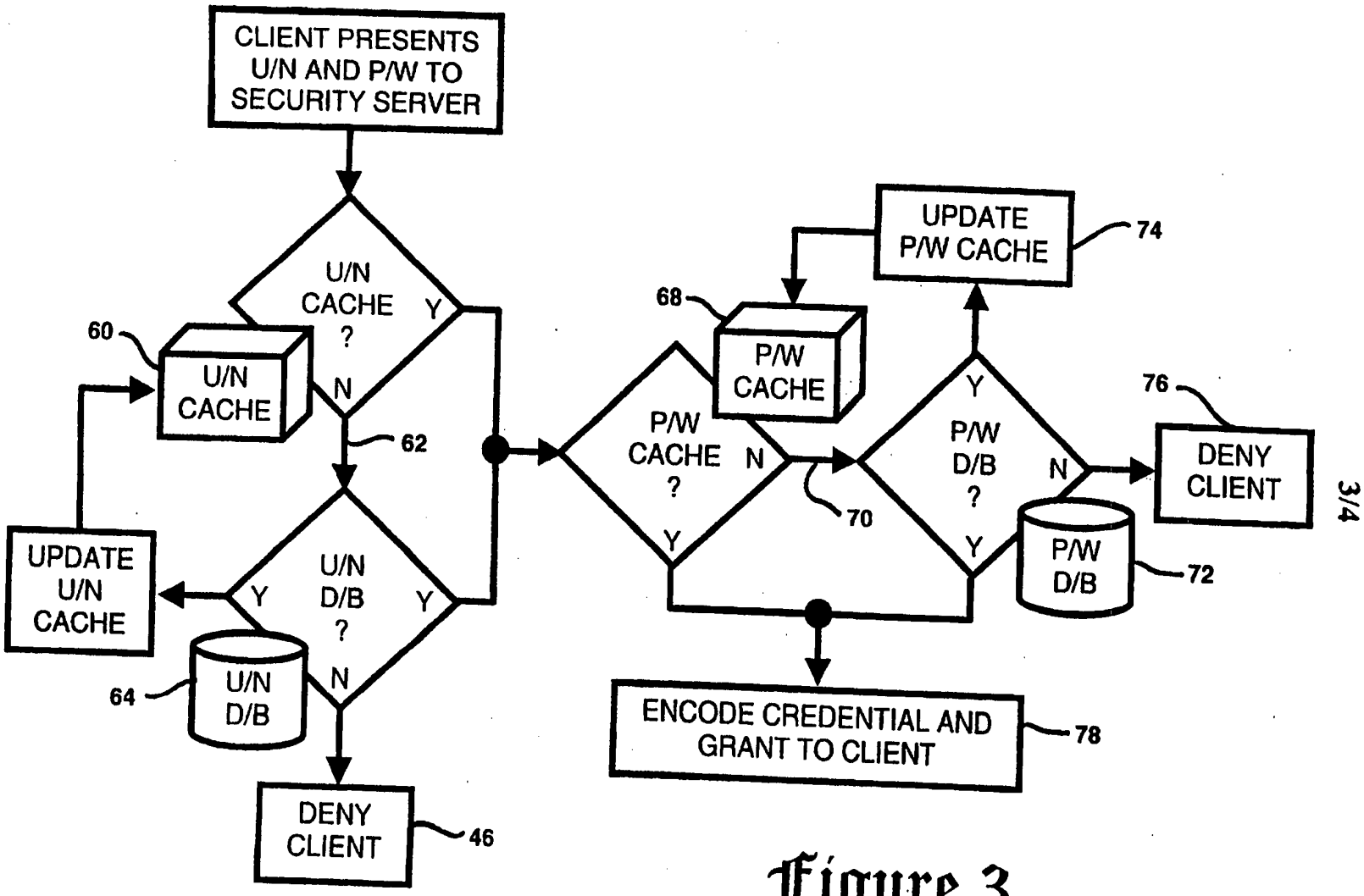
CLIENT PRESENTS U/N AND P/W TO SECURITY SERVER
U/N CACHE ?
Y
N
60
U/N CACHE
62
UPDATE U/N CACHE
U/N D/B ?
Y
Y
N
64
U/N D/B
DENY CLIENT
46
68
P/W CACHE
P/W CACHE ?
N
Y
70
UPDATE P/W CACHE
74
P/W D/B ?
Y
N
Y
76
DENY CLIENT
P/W D/B
72
ENCODE CREDENTIAL AND GRANT TO CLIENT
78

Figure 3

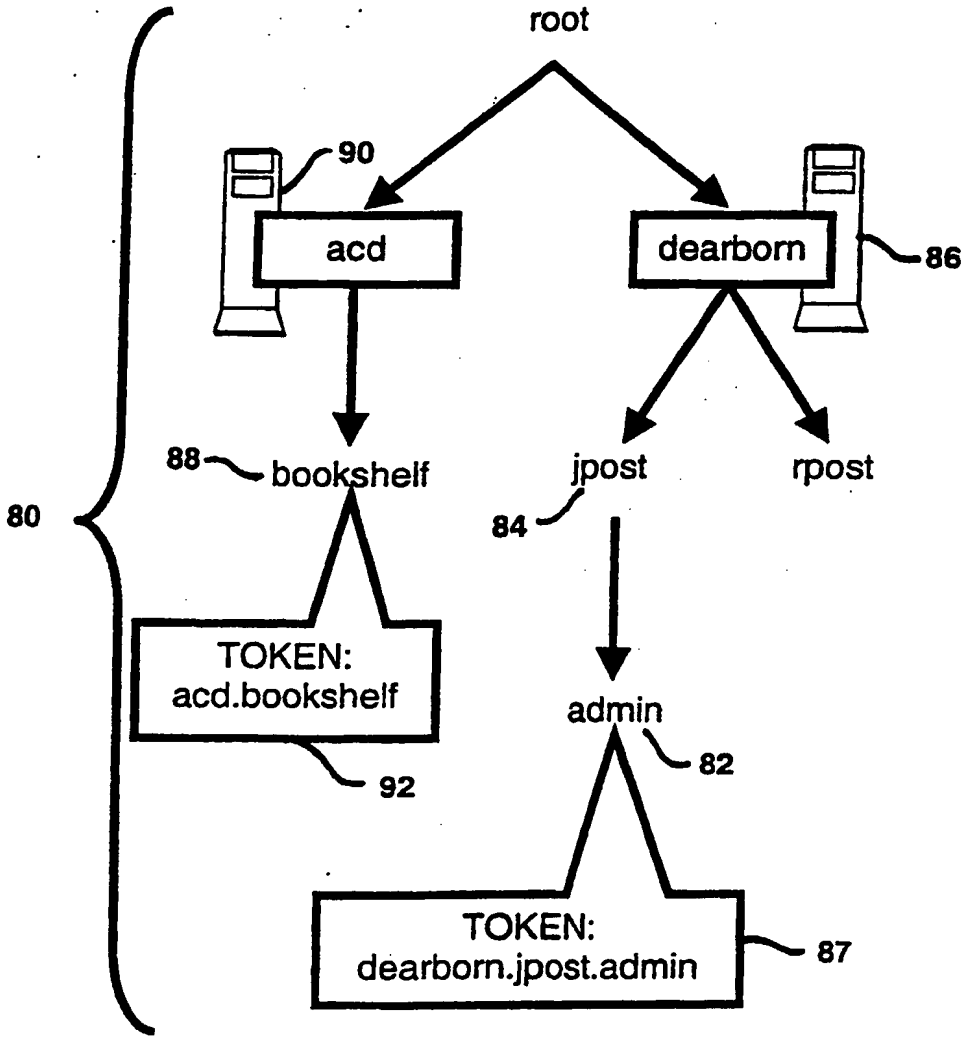
root
90
acd
dearborn
86
88
bookshelf
jpost
rpost
80
84
TOKEN:
acd.bookshelf
admin
92
82
TOKEN:
dearborn.jpost.admin
87

Figure 4

A METHOD AND SYSTEM FOR GLOBALLY RESTRICTING CLIENT ACCESS TO A SECURED WEB SITE

This invention relates generally to restricting access to a web site via single client logon and, more particularly, to a method and system for globally restricting client access to a secured web site based on role-based access credential attributes specific to the client.

Today, many corporate entities rely extensively on web-based applications and informational resources to carry out their critical business activities. For example, a single manufacturing company may rely internally on web-based accounting, personnel, inventory and production applications. Externally, the company may purchase from and sell to hundreds of distributed suppliers communicating and executing purchase orders via the manufacturer's web-based purchasing and selling application.

To maintain an adequate level of integrity, business critical applications must be secured by competent access authorization validation solutions. Conventionally, each site developer creates his or her own solution to meet the security needs of the site or application owner. No standard security mechanism exists for globally defining access to web sites and web-based applications. Site or application owners that wish to restrict client access in any manner have to define, assign and manage unique passwords for every potential client user.

From the client users' perspective, password management is overwhelming as well. Most client users have to remember a unique password and login ID for each of the secured applications they utilize in their everyday business activities. As companies continue to streamline and secure business information on a web-based platform, the number of

login IDs and passwords the average employee must remember increases.

To alleviate the site owners' burden of managing passwords and corresponding site access authorizations, site owners need a method and system for globally defining access among groups of clients having the application in common. For example, the administrator of a corporate purchasing application should be able to globally authorize all purchasing department employees or external suppliers to access his application. This global role-based authorization eliminates the need of defining, assigning and managing unique passwords for every potential client user.

To alleviate the client user's burden of remembering an overwhelming number of user IDs and corresponding passwords, the method and system should allow authorized clients to access the secured sites and applications utilizing a cookie-based access credential in lieu of a conventional user name and password login. Such a solution would require a client to authenticate him or herself via single logon to a security server transparent to the server hosting the secured application. Preferably, the security server allocates the corporate role-based access credentials to clients based on synchronized databases of pre-existing client passwords (e.g., Microsoft Outlook, Windows NT and LDAP-compliant directories, etc.).

It is an object of the invention to provide a method and system for globally restricting client access to a secure web site.

According to a first aspect of the invention there is provided a system for globally restricting client access to a secured web site comprising a first web server configured to

receive a client login and return a cookie to the client containing an access credential wherein the access credential contains at least one role-based attribute specific to the client and a second web server hosting a secured web site having an associated security expression wherein the security expression contains at least one role-based access privilege for the web site, the second web server configured to receive the cookie containing the access credential in response to an HTTP request from the client and if the access credential contains a role-based attribute in common with the security expression, grant the client access to the secured web site.

Preferably, the access credential and security expression may additionally contain a token attribute for locally defined access to the secured web site.

The token attribute may contain permission re-granting capability.

The access credential may be digitally signed.

Preferably, role based attributes may be assigned to the client based on the client's login password.

The first web server may be additionally configured to synchronize client passwords among more than one password repository.

The web site may contain a web-based application.

The access credential may expire after a predefined period of time.

The access credential may be encoded.

According to a second aspect of the invention there is provided a method for globally restricting client access to a secured web site comprising receiving a client login at a first web server, returning a cookie to the client containing an access credential wherein the access credential contains at least one role-based attribute specific to the client, receiving the cookie containing the access credential from the client in response to an HTTP request at a second web server wherein the second web server hosts a secured web site having an associated security expression containing at least one role-based access privilege and if the access credential contains a role-based attribute in common with the security expression, granting the client access to the secured web site.

The access credential and security expression may additionally contain a token attribute for locally defined access to the secured web site.

The token attribute may contain permission re-granting capability.

The access credential may be digitally signed.

Preferably, role based attributes may be assigned to the client based on the client's login password.

The first web server may be configured to synchronize client passwords among more than one password repository.

The web site may contain a web-based application.

The access credential may expire after a predefined period of time.

The access credential may be encoded.

The invention will now be described by way of example with reference to the accompanying drawing of which:-

Figure 1 is a block flow diagram illustrating a preferred method for carrying out the present invention;

Figure 2 illustrates the environment in which the present invention operates;

Figure 3 is a block flow diagram illustrating the secured server response to a client login; and

Figure 4 is a tree diagram illustrating a hierarchal relationship among example token attributes in accord with the present invention.

The present invention comprises a method and system for controlling access to a plurality of secured web sites or web-based applications via single client logon. Figure 1 is an overview block flow diagram illustrating a preferred method for carrying out the invention. Figure 2 illustrates a system for restricting access to a web site or application in accord with the present invention.

Referring to Figures 1 and 2, a site owner 40 publishes a web site 42 (or web-based application) to a hosting server 44 as described in block 10. To define which clients 46 are entitled to access the site, the site owner defines a security file 50 for the web site, as described in block 12. Security expression definition is discussed in more detail infra.

To access the secured site 42, a client 46 presents the hosting server 44 with an HTTP request as described in block 14. In response to the HTTP request, the hosting server 44 retrieves a cookie from the client containing an encoded access credential 52. If the client is accessing the secured site for the first time, the hosting computer will

be unable to retrieve the necessary cookie as indicated by arrow 16 and will automatically redirect the client to a security server 48 as described in block 18.

Upon redirect to the security server 48, the client 46 is presented with a conventional login request 49 comprising a user name and password as described in block 20. Figure 3 is a block flow diagram illustrating the security server response to the client login. After receiving the client's user name and password, the security server queries a user name cache 60 for a user name matching the user name input by the client. If no match is found within the user name cache as indicated by arrow 62, the security server queries a user name database 64 for a user name matching the user name input by the client. If no match is found within the user name database, the client is denied access to the secured site 42 as described in block 65.

If a user name match is found within the user name database 64, the user name cache 60 is updated and the security server queries a password cache 68 for a password matching the password input by the client. If no match is found within the password cache as indicated by arrow 70, the security server queries a password database 72 for a password matching the password input by the client. If no match is found within the password database, the client is denied access to the secured site 42 as described in block 76. If a match is found within the password database 72, the password cache 68 is updated to include the client's password as described in block 74.

In accord with a preferred embodiment of the present invention, the password database 72 provides password synchronization among a plurality of password repositories (e.g., Microsoft Outlook, Microsoft Windows NT and lightweight directory access protocol-compliant directories (LDAP), etc.).

Referring again to Figures 1 and 2, clients having a valid user name and password are each granted a cookie containing a unique encoded access credential 52 as described in block 78.

In accord with the preferred embodiment of the present invention, each access credential 52 comprises at least one attribute. Generally, access credential attributes can be divided into three categories: time-sensitive, corporate role-based, and token-based.

Time sensitive access credential attributes comprise issue date and expiration date (e.g., ten hours from issue date). Corporate role-based access credential attributes comprise issuer, user identification, Internet protocol (IP) address, group name, department name, organization code, employee type, management role, organization name, common name, division abbreviation, building code, building city, building state, building country and authorization type. Token-based access credential attributes are discussed in more detail infra.

A hash algorithm (e.g., RSA Security MD5) is used to provide integrity for the present invention. Authenticity for the present invention is provided using a public key algorithm (e.g., the RSA security RSA public key algorithm). The security server 48 contains the private key and the corresponding public key is contained within the hosting server 44.

After receiving a valid cookie containing an encoded access credential 52 from the security server 48, the client 46 is automatically redirected to the hosting server 44 as described in block 22.

In response to the redirected HTTP request at the secured site 42, the hosting server 44 retrieves the cookie containing the encoded access credential, distils the encoded access credential and decodes the access credential as described in block 24. Next, the decoded access credential is compared to the security file 50 having to determine whether the client is authorized to access the secured site as described in blocks 28 and 30.

For each site 42 hosted on the hosting server 44, the corresponding site owner 40 defines a security file containing various parameters and rules that define which users are authorized to access the secured site or application. Authorization is accomplished via a standard agent for NSAPI & ISAPI installed on the hosting server and granularity is to the directory level.

On the UNIX platform, the name of the security file is ".wslauth" On the Windows NT platform, the name of the security file is "auth.wsl". The standard syntax for the security expression within the security file is: security="security expression".

Table 1 contains the security file syntax in accordance with the present invention.

Table 2 defines special characters for defining security expressions in accordance with the present invention.

Table 3 contains security files having example security file expressions.

Security File Syntax	Access Privileges
security="off" or security="none"	all users (disables access control)
security="attribute:value"	users matching the attribute value
security="attribute!value"	users not matching the attribute value
security="$:token"	users possessing the token, discussed infra

Table 1 - Security File Syntax

Character	Name	Meaning
|	pipe	or
,	comma	and
!	exclamation	not equal
:	colon	equal
*	asterisk	wildcard matches zero or more characters
?	question	wildcard matches exactly one character
()	parenthesis	for grouping conditionals

Table 2 - Special Characters

Unlike role-based access credential attributes (e.g., group name, department name, organization code, etc.), the "token" access credential attribute 45 allows a site owner 40 to locally allocate site access to particular users/clients 46 or groups of users/clients as indicated by arrow 47.

Security File	Access Privileges
security= "empcode:F|empcode:A|empcode:J"	All users having an F, A or J "employee code" access credential attribute
security= "user:prathbun|user:mkromer"	P. Rathbun and M. Kromer, as identified by the user attribute within their respective "user" access credential attributes
security= "$:dearborn.wsl.example"	All users that have the dearborn.wsl.example "token" access credential attribute
security= "$:dearborn.wsl.example|user:prathbun"	All users that have the dearborn.wsl.example "token" access credential attribute or P. Rathbun, as identified by his "user" access credential attribute
security="mmrole:Y"	All users that possess the "management role" access credential attribute

Table 3 - Security Files with Example Security Expressions

In accord with a preferred embodiment of the present invention, tokens are defined in a compounded format following an inverted group relationship. Figure 4 illustrates an example hierarchal relationship 80 between tokens. According to the example, a user 80 with "admin" permission for the "jpost" application 84 on the "dearborn" server 86 is allocated a "dearborn.jpost.admin" token 87. Similarly, a user with access to the "bookshelf" application 88 on the "acd" server 90 is allocated an "acd.bookshelf" token 92.

Special tokens called token-administrating tokens allow a site owner 40 to allocate tokens having access permission re-granting capability. Token-administrating tokens have a "/create" or "/grant" suffix. The "/create" context allows a user in possession of the token to create a new administrator, or to generate a new token having the same prefix as the token-administrating token. The "/grant" context allows a user in possession of the token to grant a token containing identical access privileges to another user.

Table 4 contains a variety of token users each in possession of a unique token-administrating token.

Token User	Token Syntax	Explanation
Web Site Administrator	*./create	Can create any new token for another user that ends with a ".", a "./create" or a "./grant".
Application Administrator	application.*.create	Can create any new token for another user that begins with "application." and ends with a ".", a "./create" or a "./grant".
Application Administrator	application.user./grant	Can grant "application.user" permission to any user.

Table 4 - Token-Administrating Tokens

Notably, a plurality of sites or applications 42, each having a unique site owner 40 and corresponding security

file 50 may be hosted on the hosting server 44. In an alternate embodiment, a plurality of hosting servers 44 each host at least one Web site or application 42 having a unique site owner 40 and corresponding security file 50.

While the best mode for carrying out the invention has been described in detail, those familiar with the art to which this invention relates will recognize various alternative designs and embodiments for practicing the invention as defined by the following claims.

Claims

1. A system for globally restricting client access to a secured web site comprising a first web server configured to

receive a client login and return a cookie to the client containing an access credential wherein the access credential contains at least one role-based attribute specific to the client and a second web server hosting a secured web site having an associated security expression wherein the security expression contains at least one role-based access privilege for the web site, the second web server configured to receive the cookie containing the access credential in response to an HTTP request from the client and if the access credential contains a role-based attribute in common with the security expression, grant the client access to the secured web site.

2. A system as claimed in claim 1 wherein the access credential and security expression additionally contain a token attribute for locally defined access to the secured web site.

3. A system as claimed in claim 2 wherein the token attribute contains permission re-granting capability.

4. A system as claimed in claim 1 wherein the access credential is digitally signed.

5. A system as claimed in any of claims 1 to 4 wherein role based attributes are assigned to the client based on the client's login password.

6. A system as claimed in any of claims 1 to 5 wherein the first web server is additionally configured to synchronize client passwords among more than one password repository.

7. A system as claimed in any preceding claim wherein the web site contains a web-based application.

8. A system as claimed in any preceding claim wherein the access credential expires after a predefined period of time.

9. A system as claimed in any preceding claim wherein the access credential is encoded.

10. A method for globally restricting client access to a secured web site comprising receiving a client login at a first web server, returning a cookie to the client containing an access credential wherein the access credential contains at least one role-based attribute specific to the client, receiving the cookie containing the access credential from the client in response to an HTTP request at a second web server wherein the second web server hosts a secured web site having an associated security expression containing at least one role-based access privilege and if the access credential contains a role-based attribute in common with the security expression, granting the client access to the secured web site.

11. A method as claimed in claim 10 wherein the access credential and security expression additionally contain a token attribute for locally defined access to the secured web site.

12. A method as claimed in claim 11 wherein the token attribute contains permission re-granting capability.

13. A method as claimed in any of claims 10 to 12 wherein the access credential is digitally signed.

14. A method as claimed in any of claims 10 to 13 wherein role based attributes are assigned to the client based on the client's login password.

15. A method as claimed in any of claims 10 to 14 wherein the first web server is configured to synchronize client passwords among more than one password repository.

16. A method as claimed in any of claims 10 to 15 wherein the web site contains a web-based application.

17. A method as claimed in any of claims 10 to 16 wherein the access credential expires after a predefined period of time.

18. A method as claimed in any of claims 10 to 17 wherein the access credential is encoded.

19. A system for globally restricting client access to a secured web site substantially as described herein with reference to the accompanying drawing.

20. A method for globally restricting client access to a secured web site substantially as described herein with reference to the accompanying drawing.

INVESTOR IN PEOPLE

Application No: GB 0208436.6 **Examiner:** Geoff Western
Claims searched: All **Date of search:** 21 October 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4A (AAP)

Int Cl (Ed.7): G06F 1/00, 12/14

Other: Online: JAPIO, EPODOC, WPI, TDB, INSPEC, XPESP, IEEEXplore

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
Y	EP 1089516 A2	(CITICORP) N.b. paras 6-9	1,4,7-10,13,16-18
Y	EP 0992145 A1	(BRITISH TELECOM) N.b. pages 1-3	1,4,7,9,10,13,16,18
Y,P	WO 2002/012987 A2	(ASSOCIATES THINK) N.b. paras 32,33, claims	1,4,7,9,10,13,16,18
Y	WO 2001/025882 A1	(SIMPSON) N.b. pages 3-9	1,4,7,9,10,13,16,18
Y,P	US 6339423 A	(BELMONTE et al) N.b. columns 2,3	1,4,7,9,10,13,16,18

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.